00144 ***Roma, data del protocollo***

Ministero delle Infrastrutture e dei Trasporti

Comando generale
del Corpo delle capitanerie di porto

Reparto 6° - Ufficio 2° - Sezione 1ª

Al **VDS ELENCO INDIRIZZI ALLEGATO**

CIRCOLARE TITOLO:
SICUREZZA DELLA NAVIGAZIONE

Serie Generale: 155/2019

Argomento: **Cyber risk management.**

Riferimenti:
- Circolare titolo Security n.35/2017;
- Circolare Non di Serie n.8/2018.

Il mondo della comunicazione a distanza nasce nel 1844 quando Samuel Finley Breese Morse brevettò il telegrafo elettrico, un apparecchio in grado di inviare messaggi a grandi distanze[1].

Da allora la tecnologia si è evoluta in maniera sorprendente determinando significativi vantaggi in termini di efficienza in tutti i settori, ivi incluso quello marittimo, presentando al contempo notevoli rischi legati alla potenziale vulnerabilità dei processi informatici dedicati al funzionamento dei vari sistemi.

Nel giugno 2017 l'impatto di tali rischi è stato avvertito in modo significativo a seguito dell'attacco informatico perpetrato a livello internazionale da parte di *hacker* che hanno reso inaccessibili i sistemi informatici di molte imprese e coinvolgendo, anche, il comparto dello *shipping.*

Per rispondere a tali pericoli e procedere ad una corretta gestione del rischio informatico, il 16 giugno 2017 l'International Maritime Organization (IMO) ha adottato le raccomandazioni contenute nella Risoluzione MSC.428(98) "*Maritime Cyber Risk Management in Safety Management Systems",* attraverso le quali è stato determinato che la valutazione del rischio informatico, oltre ad essere divenuto elemento essenziale, rientra tra gli obiettivi del Codice ISM e ricade tra rischi generali che possono interessare ed impattare sulla sicurezza della nave, del personale e dell'ambiente.

[1] Il primo messaggio ufficialmente trasmesso in morse diceva: *"Guardate che cosa ha saputo fare il Signore Iddio"* L'ultimo mestamente diceva: *"Chiamiamo tutti. Questo è il nostro ultimo grido prima del silenzio eterno" (Stazione francese di La Conquette verso l'Atlantico – 24.00 del 31.1.1997)*

Alla luce di quanto determinato in sede IMO è quindi necessario garantire che i rischi cibernetici siano adeguatamente analizzati e mitigati nell'ambito del SMS, con corrispondente emendamento del proprio sistema di gestione, e verificati in occasione della prima verifica annuale del *Document of Compliance* (DOC) **dopo il 1° gennaio 2021**.

Il 5 luglio 2017, l'IMO ha quindi pubblicato un secondo documento, la MSC-FAL.1/Circ.3 "*Guidelines on maritime cyber risk management*", recante una serie di raccomandazioni di carattere generale, in cui vengono individuate le possibili vulnerabilità dei sistemi – distinguendo le "*information e operational technology*" – e definendo, quale ulteriore obiettivo, la protezione dello scambio di informazioni e dati. Particolare importanza viene attribuita alla valutazione della vulnerabilità attraverso una necessaria comparazione tra progettazione, integrazione e/o manutenzione dei sistemi per la definizione di eventuali vuoti/errori nella c.d. *cyberdiscipline.*

È altrettanto evidente che le rapide modifiche tecnologiche e le relative minacce rendono difficile indirizzare i rischi solo attraverso standard tecnici. Le linee guida, pertanto, raccomandano una gestione del rischio cibernetico attraverso un "*risk management approach*"; il rischio cibernetico è da considerarsi quale "naturale" evoluzione ed estensione delle già esistenti "*management practices*" in campo safety e security.

Risulta opportuno quindi definire il "*cyber risk management*" che l'IMO ha identificato quale "processo di identificazione, analisi, verifica e comunicazione di un *cyber-related risk* accettando, evitando, trasferendo o mitigando lo stesso rischio ad un livello accettabile e considerando costi/benefici delle azioni da intraprendere".

Tale operazione può essere svolta attraverso una globale verifica e comparando l'attuale organizzazione, quella desiderata e i risultati (*posture*) del cyber risk management. Tale comparazione potrebbe rilevare mancanze (*gaps*) che dovrebbero quindi essere valutate al fine di raggiungere gli obiettivi del *risk management* anche attraverso un piano di prioritizzazione dei rischi. La stessa MSC-FAL.1/Circ.3 indica quelli che sono considerati i c.d. *functional elements* utili per supportare un efficace *cyber risk management* la cui finalità è quella di assicurare un adeguato livello di *awareness* del *cyber risk* a tutti i livelli dell'organizzazione ed essere commisurato in considerazione dei ruoli e delle responsabilità di ogni elemento parte del sistema.

Inoltre, in tale contesto, si evidenzia quanto emerso durante il MSC 101 in cui si è chiarito che gli aspetti della gestione del rischio informatico, compresa la sicurezza fisica, dovrebbero essere considerati anche nei Piani di Security delle navi (SSP) ai sensi del codice ISPS fermo restando – per tutto quanto sopra richiamato - che non deve essere considerato obbligo per le Società di gestione istituire un sistema di gestione separato della sicurezza informatica che operi in parallelo con il sistema SMS adottato. Il Piano di Security della nave (SSP) farà però riferimento alle procedure di gestione dei rischi informatici presenti nel citato SMS ed il loro trattamento (come meglio descritto nell'annesso) avverrà qualora emergano necessità in sede di valutazione e come tra l'altro già si evince dalla lettura comparata della normativa vigente ed in particolare:

- dell'ISM code, adottato dal Cap. IX SOLAS, punto 1.2.2.2: "*assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards*"; e
- dell'ISPS Code, adottato dal Cap. XI-2 SOLAS, Parte B punto 8.5.3: "*radio and telecommunication systems, including computer systems and networks*".

Nel contesto cyber security, appare inoltre utile richiamare, che lo scrivente Reparto ha proceduto, con la Circolare titolo Security n.35/2017, ad eseguire un primo censimento concernente il *cyber risk management* i cui risultati sono stati resi noti con la Circolare Non di Serie n.8/2018.

Per tutto quanto sopra, lo scrivente Reparto, su condiviso parere del Gruppo di lavoro in materia di sicurezza della navigazione integrato da un rappresentante dell'Autorità NIS, ritiene necessario che le Società si dotino di un *risk management framework.*

Tale *risk management framework* deve tenere in debita considerazione gli elementi di cui all'annesso della presente Circolare – parte integrante della stessa - nonché la Risoluzione MSC.428(98), la MSC-FAL.1/Circ.3 e le disposizioni impartite dall'Autorità NIS alle Società che sono state classificate Operatori di Servizi Essenziali (OSE).

Gli aggiornamenti al Sistema di gestione della sicurezza (SMS) devono essere verificati ai sensi del punto 6 "*Manuale del safety management*" della Circolare Serie Generale 69/2007.

IL CAPO REPARTO
CA (CP) Luigi GIARDINO
(documento sottoscritto con firma digitale,
ai sensi del D.lvo 82/2005 n.21)

Firmato digitalmente da
LUIGI GIARDINO
O = CAPITANERIE DI PORTO - GUARDIA COSTIERA
C = IT

Ministero delle Infrastrutture
e dei Trasporti

Comando generale
del Corpo delle capitanerie di porto
Reparto 6° - Sicurezza della navigazione

Annesso

Circolare Titolo “Sicurezza della Navigazione”

Serie Generale: n.155/2019

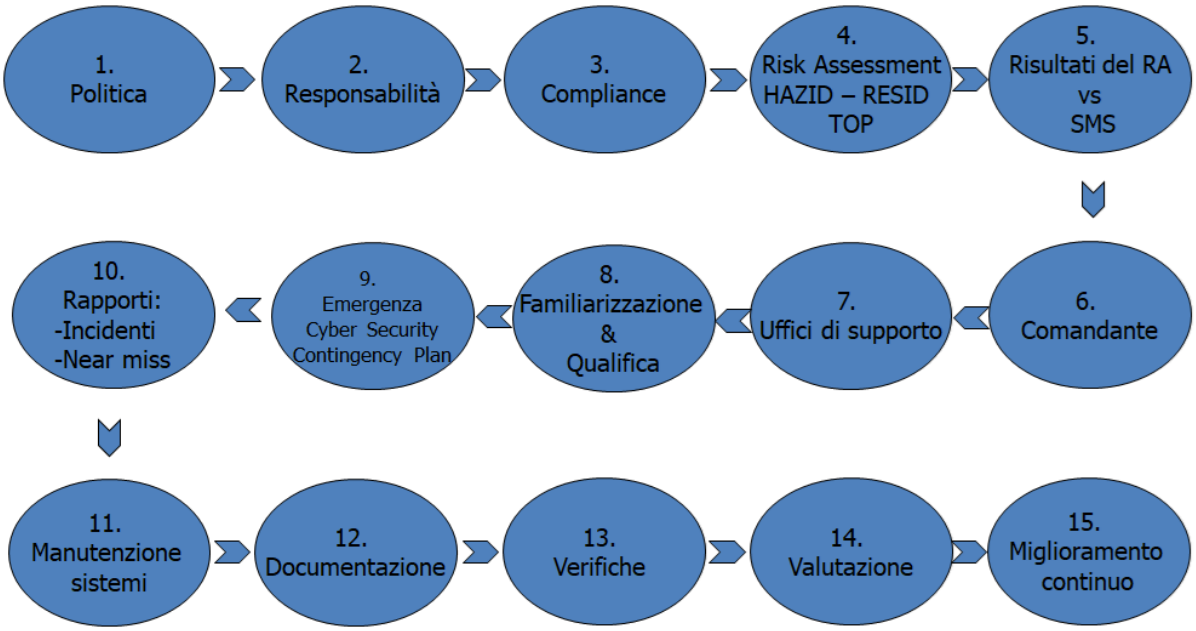
Cyber risk management

Scopo

Scopo del presente annesso è quello di identificare il processo ISM legato alla cyber security e fornire una guida che possa supportare le Società di gestione nella redazione del "*risk assessment*" (punti 4 e 5 del processo ISM) ed al fine di proteggere i sistemi e le informazioni dalle minacce informatiche.

Quanto sopra con l'obiettivo di adottare tutte le misure per garantire, ai sensi del codice ISM (punto 1 del preambolo), la gestione sicura della nave, la protezione dell'ambiente e la tutela dell'equipaggio.

Processo ISM



1. POLITICA (Codice ISM punto 2.1) - La politica della Company dovrà essere modificata (ampiamento dei propri obiettivi di gestione ISM) con l'inserimento degli aspetti di cyber security e le misure necessarie ai fini della sicurezza della nave legata anche ai rischi cyber.

2. RESPONSABILITA' (Codice ISM punto 3.2) - La Company deve designare, a terra, un responsabile per la gestione e protezione contro i rischi informatici che possa fornire assistenza al Comandante della nave per lo svolgimento dei suoi compiti.

3. COMPLIANCE (Codice ISM punto 1.2) - linee guida e raccomandazioni dell'IMO (punto 4.2. della MSC-FAL.1/Circ.3), dell'Amministrazione e degli Organismi riconosciuti costituiscono una base per la creazione e l'aggiornamento del Risk Assessment (RA) e dell'aggiornamento SMS della Company. Gli aggiornamenti/modifiche al Sistema di gestione della sicurezza (SMS) devono essere verificati ai sensi del punto 6 "*Manuale del safety management*" della Circolare Serie Generale 69/2007
4. RISK ASSESSMENT (Codice ISM punto 1.2) - Risk Assessment dovrà individuare i rischi, le protezioni contro gli attacchi e le responsabilità e tenendo in debita considerazione la Circolare SG 83/2010.
   Nello sviluppo del RA è necessario considerare i diversi sistemi operativi (Operational Technology System - OT) e quelli informatici (Information Technology System- IT)[2].
   Le tipiche differenze fra IT ed OT sono riportate nella tabella in Allegato A[3].

[2] I sistemi OT (hardware e software) monitorano/controllano direttamente i dispositivi fisici e i processi, mentre i sistemi IT gestiscono i dati.

[3] di cui alla "*Guidelines on Cyber Security Onboard Ships*" prodotta da BIMCO, CLIA, ICS, INTERCARGO INTERTANKO, OCIMF e IUMI e sue successive modifiche ed integrazioni

Inoltre, dovranno essere almeno inclusi gli aspetti previsti dal punto 3.5 della MSC-FAL.1/Circ.3 che, per comodità di illustrazione, si riportano di seguito:

a. Identificazione: definire ruoli e responsabilità ed identificare pericoli e sistemi critici (Allegato B^2). Per una valutazione sistematica potranno essere utilizzati:
    1. Identificazione dei pericoli (HAZID): necessario creare un elenco senza valutazione e determinazione del rischio con tutti i potenziali pericoli e le risorse potenzialmente a rischio (Esempi in Allegato C); e
    2. Identificazione delle risorse (RESID): individuare un elenco di risorse sia interne che esterne (per esempio produttori e tecnici per la protezione di OT e IT potrebbero dover essere coinvolti se le risorse proprie non sono sufficienti. L'elenco RESID dovrebbe identificare quale risorsa diventa necessaria – (Esempi in Allegato D);
b. Protezione: protezione dagli attacchi (Allegato E^2) attraverso misure tecniche (T), organizzative (O) e personali (P) – (Esempi in Allegato F);
c. Rilevazione: Individuazione di un attacco in modo tempestivo (Allegato G^2);
d. Risposta: Misure per rispondere ad un attacco (Allegato H^2);
e. Ripristino: Misure da eseguire dopo un attacco (Allegato I^2).

5. RISULTATI DEL RA – I risultati del RA dovranno essere registrati come processi e le misure adottate dovranno essere rese note all'equipaggio. Se il RA stabilisce che determinate misure non dovrebbero essere rese pubbliche o non dovrebbero rivolgersi a tutte le persone all'interno della Società di gestione, allora le stesse dovranno essere parte della valutazione del rischio (SSA) e del piano di sicurezza della nave (SSP).

6. COMANDANTE (Codice ISM punti 6.1, 6.2) - Il SMS dovrà riportare le procedure indirizzate al Comandante della nave. In questo la Società deve anche tenere conto che nuovi compiti di cyber non sono esclusivamente responsabilità del Comandante ma distribuiti in considerazione degli incarichi e delle responsabilità (terra e bordo).

7. UFFICI DI SUPPORTO - Il Comandante deve ricevere un supporto qualificato da terra al fine di porre in essere le misure e i compiti previsti in materia di *cybersecurity*. Questo supporto deve almeno prevedere come rispondere ad un attacco di cyber, cosa fare a seguito di un attacco e come ripristinare i servizi dopo un attacco.

8. FAMILIARIZZAZIONE (Codice ISM punti 6.3, 6.5) - I membri dell'equipaggio ed il personale dell'ufficio devono familiarizzare con le misure di sicurezza informatica. Familiarizzazione, istruzione ed ulteriori misure di formazione devono essere periodicamente ripetute. L'SMS dovrà contenere un piano di formazione e descrivere le misure per determinare le esigenze di formazione per i marittimi ed il personale di terra in relazione alla propria posizione ricoperta.

9. EMERGENZA (Codice ISM punti 8.1, 8.2) - L'SMS deve contenere un "*cyber security contingency plan*" che deve essere messo in pratica attraverso esercitazioni, simulazioni e training. I piani devono almeno includere le misure per rispondere ad un attacco cyber, alle sue conseguenze e le necessarie misure di backup.

10. RAPPORTI (Codice ISM punti 9.1, 9.2) - Gli incidenti, i mancati incidenti ed altri eventi rilevanti dovranno essere segnalati ai responsabili della Company di cui al punto 2 utilizzando le procedure previste dal manuale SMS.

11. MANUTENZIONE DEI SISTEMI (Codice ISM punti 10.1, 10.2, 10.3) - Le misure di sicurezza che sono state identificate dal RA come ricorrenti devono essere inserite nel sistema di manutenzione pianificato che monitora e documenta tali misure. (es: aggiornamenti software)

12. DOCUMENTAZIONE (Codice ISM punto 11) - Se le misure individuate e i requisiti previsti rientrano nel campo dei dati sensibili, misure specifiche dovrebbero essere attuate al fine di renderle accessibili solo ad un gruppo limitato di persone a bordo e a terra. (Esempi: diritti di amministratore a bordo e gestione password, gestione backup e ripristino.)
13. VERIFICHE (Codice ISM punto 12.1) – L'implementazione della gestione della sicurezza informatica nel sistema ISM aziendale e il continuo aggiornamento sono monitorati e verificati da audit e revisioni. Gli audit interni devono essere eseguiti a bordo e presso l'ufficio a intervalli non superiori a 12 mesi.
14. VALUTAZIONE (Codice ISM punti da 12.2 a 12.7) - La Società verifica e valuta regolarmente il sistema di gestione della sicurezza rispondendo almeno alle seguenti domande:
    - L'organizzazione (Bordo e terra) funziona secondo i requisiti SMS?
    - Le misure dell'SMS sono efficaci?
    - I revisori interni sono qualificati in sicurezza informatica?
    - I risultati degli audit sono portati all'attenzione del personale competente?
    - Le misure correttive e preventive necessarie sono avviate/implementate tempestivamente?
15. MIGLIORAMENTO CONTINUO - La Company deve tenere conto dei cambiamenti costanti e delle debolezze identificate nel proprio sistema e garantire l'aggiornamento del sistema di valutazione dei rischi e del SMS, avviando così il processo di miglioramento continuo.

Allegato A

Category	IT system	OT system
Performance requirements	■ non-real-time ■ response must be consistent ■ less critical emergency interaction ■ tightly restricted access control can be implemented to the degree necessary for security	■ real-time ■ response is time-critical ■ response to human and any other emergency interaction is critical ■ access to OT should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (reliability) requirements	■ responses such as rebooting are acceptable ■ availability deficiencies may be tolerated, depending on the system's operational requirements	■ responses such as rebooting may not be acceptable because of operational requirements ■ availability requirements may necessitate back-up systems
Risk management requirements	■ manage data ■ data confidentiality and integrity is paramount ■ fault tolerance may be less important. ■ risk impacts may cause delay of: ship's clearance, commencement of loading/ unloading, and commercial and business operations	■ control physical world ■ safety is paramount, followed by protection of the process ■ fault tolerance is essential, even momentary downtime may not be acceptable ■ risk impacts are regulatory non-compliance, as well as harm to the personnel onboard, the environment, equipment and/or cargo
System operation	■ systems are designed for use with commonly known operating systems ■ upgrades are straightforward with the availability of automated deployment tools	■ differing and possibly proprietary operating systems, often without built in security capabilities ■ software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and possible involvement of modified hardware and software
Resource constraints	■ systems are specified with enough resources to support the addition of third-party applications such as security solutions	■ systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities

Roles and responsibilities[21]	
Action	**Remarks**
ISM Code: 3.2 Industry Guidelines: 1.1 Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.	An updated safety and environment protection policy should demonstrate: ■ a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment ■ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks ■ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.
ISM Code: 3.3 Industry Guidelines: 1.1 Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).	In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[22] onboard ships and are responsible for the SMS. Allocation of responsibility and authority may need to be updated to enable CRM. This should include: ■ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel ■ incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
ISM Code: 6.5 Industry Guidelines: 5.2 Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.	Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for: ■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures ■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations	
Action	**Remarks**
ISM Code: 10.3 Industry Guidelines: 3 & 4 Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.	An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS. However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).

Allegato C

HAZID HAZard IDentification			
IT **Sistemi informatici e reti**	**Interfaccia**	**OT** **Sistemi operativi**	**Punti di accesso**
PC d'ufficio **Email** **Internet** **Telefoni (incluso satellitari)** **Server** **WLAN/LAN** **PC carico** **PC stabilità** **…**	**IT e OT**	**GNSS** **AIS** **RADAR** **ECDIS** **Sistemi di controllo apparato motore** **Allarmi** **Monitoraggio** **…**	**USB** **LAN** **WLAN** **DVD/CD ROM** **…**

Allegato D

RESID RES IDentification			
IT **Sistemi informatici e reti**	**Interfaccia**	**OT** **Sistemi operativi**	**Punti di accesso**
Competenza: interna o esterna? **Se del caso elencare tutti i produttori e possibili servizi in appalto** **…**	**IT e OT**	**Competenza: interna o esterna?** **Se del caso elencare tutti i produttori e possibili servizi in appalto** **…**	**Competenza: interna o esterna?**

Implement risk control measures	
Action	**Remarks**
ISM Code: 1.2.2.2 Industry Guidelines: 5 and Annex 1 Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.	The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines. As a baseline, the following measures should be considered before a risk assessment is undertaken. The baseline consists of the technical and procedural measures, which should be implemented in all companies to the extent appropriate. These measures are: ■ Hardware inventory – Develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. ■ Software inventory – Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for: • maintaining this inventory when hardware controlled by the company is replaced • maintaining this inventory when software controlled by the company is updated or changed • authorizing the installation of new or upgraded software on hardware controlled by the company • prevention of installation of unauthorized software, and deletion of such software if identified • software maintenance. ■ Map data flows – Map data flows between critical systems and other equipment/technical systems on board and ashore, including those provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for: • maintaining the map of data flows to reflect changes in hardware, software and/or connectivity • identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware • reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance • controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems. ■ Implement secure configurations for all hardware controlled by the company – This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company. ■ Audit logs – Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for: • policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine • procedures for the collation and retention of security logs by the company, if appropriate. ■ Awareness and training – See line 3 above. ■ Physical security – The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.

Develop contingency plans	
Action	**Remarks**
ISM Code: 7 Industry Guidelines: 6 Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment which rely on OT.	An approved SMS should already address procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment. In general, these plans should be unaffected by the incorporation of CRM into the SMS. This is because the effect of the loss of availability of OT, or loss of integrity of the data used or provided by such systems, is the same as if the OT was unavailable or unreliable for some other reason. Notwithstanding this, consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst any suspected disruption is investigated. Procedures for periodically checking the integrity of information provided by OT to operators should be considered for inclusion in operational maintenance routines.
ISM Code: 8.1 Industry Guidelines: 6 Update emergency plans to include responses to cyber incidents.	An approved SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into safety management systems. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment. Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary.

Allegato F

T – Misure tecniche		
Firewall Programmi antivirus Filtro antispam Firewall e software antivirus e filtro antispam installati su tutti i PC Blocco USB (memoria di massa) Archiviazione di backup (soluzione esterna) Blocco di determinati tipi di file ed email Limitazione sulla posta elettronica Gestione della configurazione Separazione di sistemi interni ed esterni VPN	Controllo dell'accesso remoto: autenticazione degli accessi Accesso dei dispositivi (USB, LAN), Reti: segmentazione multipla (Operazione/master/Crew/...), in particolare le reti WLAN (protezione aggiornata all'ultimo standard) Soluzione autonoma invece del sistema di rete (ad es. cargo-PC) Software: diversi livelli di accesso (software, drives)	Internet per l'equipaggio: soluzione autonoma anziché "networking in cabina" (separazione fisica dalla rete) File di registro per esperti IT (follow-up) la Società eviti l'utilizzo di semplici servizi cloud, altrimenti fornisca i servizi attivazione automatica degli aggiornamenti: - Software in generale - Office - Sistemi OT - Sistema IT - programma antivirus Le funzioni e i plug-in software non necessari devono essere rimossi o bloccati. Posizione del server: area riservata

O – Misure organizzative		
Politica del consiglio di amministrazione (Responsabilità) Gestione password Modifiche dinamiche (regolari) della password Assegnazione del diritto di accesso (diversi livelli) Chiare responsabilità definite a terra Designazione di un esperto IT Responsabilità a bordo Responsabilità a terra Responsabilità di terzi Servizi in appalto a bordo (autorizzazione, permesso di lavoro) Organizzazione del backup Ispezione da parte dell'IT Agli amministratori vengano assegnati solo i diritti di cui hanno bisogno	Blocco schermo (automaticamente dopo "X" minuti/manualmente all'uscita dalla postazione di lavoro) Monitoraggio e controllo: navigazione terrestre (GNSS, ECDIS) Navigazione: ridondanza, navigazione astronomica di backup Carte nautiche come backup per aree sensibili critiche ARPA errore di input di velocità Dati RADAR anziché dati AIS. Velocità: ingresso LOG anziché GPS.	Analisi e valutazione continue dei punti deboli del sistema Tutti i PC devono essere protetti e soggetti a ispezioni, in particolare i portatili Evitare competenze singole (per es. amministratore: la conoscenza può andare persa in caso di modifiche)

P – Misure personali		
Familiarizzazione iniziale Familiarizzazione programmata Familiarizzazione occasionale Training a terra Rilevazione della manipolazione del GNSS, AIS… Programmi di sensibilizzazione	Dichiarazione di omissione per manipolazione e illegale accesso alle reti Misure disciplinari in caso di inosservanza intenzionale/non intenzionale delle istruzioni Trasferimento tempestivo di informazioni ai dipendenti	Formazione su richiesta (amministratore e dipendenti) Contenuto della formazione: comportamento, monitoraggio, rilevazione, misure di risposta, gestione delle password Poster e materiale informativo

Allegato G

Develop and implement activities necessary to detect a cyber-event in a timely manner	
Action	**Remarks**
ISM Code: 9.1 Industry Guidelines: 5.1 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.	An approved SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Examples of such non-conformities and cyber incidents: ■ unauthorised access to network infrastructure ■ unauthorized or inappropriate use of administrator privileges ■ suspicious network activity ■ unauthorised access to critical systems ■ unauthorised use of removable media ■ unauthorised connection of personal devices ■ failure to comply with software maintenance procedures ■ failure to apply malware and network protection updates ■ loss or disruption to the availability of critical systems ■ loss or disruption to the availability of data required by critical systems.

Allegato H

Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event	
Action	**Remarks**
ISM Code: 3.3 Industry Guidelines: 7.1 Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.	An approved SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party. In providing the adequate resources, the following should be considered: ■ company or third party technical support should be familiar with onboard IT and OT infrastructure and systems ■ any internal response team or external cyber emergency response team (CERT) should be available to provide timely support to the DPA ■ provision of an alternative means of communication between the ship and the DPA, which should be able to function independently of all other shipboard systems, if and when the need arises ■ internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA.
ISM Code: 9.2 Industry Guidelines: 7.1 Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.	An approved SMS should already include procedures for responding to non-conformities. In general, these should not be affected by the incorporation of CRM in SMS. However, the procedures should help ensure that consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective.
ISM Code: 10.3 Industry Guidelines: 7.1 Update the specific measures aimed at promoting the reliability of OT.	An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for: ■ Software maintenance as a part of operational maintenance routines – Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person. ■ Authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks – This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session. ■ Preventing the application of software updates by service providers using uncontrolled or infected removable media. ■ Periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state. ■ Controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

Allegato I

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident	
Action	**Remarks**
ISM Code: 10.4 Industry Guidelines: 5.1 and 7.2 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for: ■ checking back-up arrangements for critical systems, if not covered by existing procedures ■ checking alternative modes of operation for critical systems, if not covered by existing procedures ■ creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident ■ maintaining back-ups of data required for critical systems to operate safely ■ offline storage of back-ups and clean images, if appropriate ■ periodic testing of back-ups and back-up procedures.

ELENCO INDIRIZZI

INDIRIZZI PER COMPETENZA	
• **CAPITANERIE DI PORTO**	**TUTTE**
• **UFFICI CIRCONDARIALI MARITTIMI**	**TUTTI**
• **UFFICI LOCALI MARITTIMI**	**TUTTI**
• **Bureau Veritas**	bvmarine_offshore@legalmail.it
• **DNV-GL**	dnvitalia@legalmail.it
• **RINA Services S.p.A.**	rina.maricogecap@legalmail.it
• **ABS Italy Srl**	absitaly@pcert.postecert.it
• **Lloyd's Register**	alberto.suri-panaioli@lr.org
INDIRIZZI PER CONOSCENZA	
• **Ministero delle Infrastrutture e dei Trasporti** *Direzione Generale per la vigilanza sulle Autorità portuali, le infrastrutture portuali ed il trasporto marittimo e per vie d'acqua interne* *SEDE*	dg.tm@pec.mit.gov.it
• **Confitarma**	confitarma@confitarma.it
• **Assarmatori**	assarmatori@pec.assarmatori.eu
• **Società non associate**	**Invio a cura del Reparto 6**
INDIRIZZI PER ESTENSIONE DI COPIA	
• **Ministero delle Infrastrutture e dei Trasporti** *Direzione Generale per le Investigazioni Ferroviarie e marittime* *SEDE*	digifema@pec.mit.gov.it
• **MARICOGECAP 2° Reparto**	**SEDE**
• **Direzione Marittima di Genova** Centro di formazione specialistica sicurezza della navigazione e trasporto marittimo del Corpo delle capitanerie di porto "C.A. (CP) Antonio DE RUBERTIS"	formazionegenova@mit.gov.it
• **ACCADEMIA NAVALE LIVORNO**	**LIVORNO**
• **MARISCUOLA TARANTO**	**TARANTO**
• **MARISCUOLA LA MADDALENA**	**LA MADDALENA**